DNA Cryptography: A Novel Approach for Data Security Using Flower Pollination Algorithm

Madhvi Popli, Gagandeep

Department of Computer Science, Punjabi University, Patiala

ARTICLE INFO

Article history:
Received 15 January 19
Received in revised form 30 January 19
Accepted 24 February 19

Keywords:
DNA Computing
DNA Cryptography
Flower Pollination Algorithm
Genetic Algorithm

ABSTRACT

The number of threats is increasing with the growth of technologies and due to extensive internet usage, it has become more difficult to provide security to important data. To overcome these issue, data encryption is necessary before sending information through transmission channel. To overcome these issues, a new technique is proposed based on the DNA cryptography along with the nature-inspired FPA algorithm. The idea behind to convert plain text to DNA strand because of its uncrackable characteristic and The FPA is considered as best and able to find effective optimized result as compared to other algorithms. In this paper, we proposed a new hybrid flower pollination algorithm with DNA cryptography. Flower pollination algorithm is a nature-inspired algorithm that helps to find the optimal solution whereas DNA cryptography helps to encrypt a large number of data in few grams of DNA. In this paper, the original form of flower pollination algorithm is presented with DNA cryptography in order to achieve optimized technique to enhance cloud security.

© 2019SUSCOM. Hosting by Elsevier SSRN. All rights reserved.
Peer review under responsibility of International Conference on Sustainable Computing in Science, Technology and Management.

1. Introduction

The modern cloud technologies have changed the perspective of architecture, development and delivery models by providing on-demand services via the internet. The US National Institute of standards and technology (NIST) defines, "Cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal effort or service providers interaction" (Mell, & Grance, 2011). With the extensive use of the internet, the risk of the number of threats is also increasing and it has become more difficult to secure important information from unwanted users. Data encryption is necessary to overcome these issues before sending information through the transmission channel. Many researchers show interest in DNA computing as it can store the adequate number of information into few grams of DNA. DNA cryptography plays a vital role in transforming important information into an encrypted form.

Optimization is a method that deals to find the extreme values of a function subject to various constraints on the variable values in order to find an optimum solution (Ravindran, et al. 2006). Optimization techniques are used to find the optimal solution by finding design variables that result in to find the best optimal solution. The gradient-based methods may be able to produce optimum results with non-linear problems but, evolutionary methods and nature-based algorithms produce optimum results in case of highly non-linear problems. Such nature-inspired methods have special rules and algorithm that have different inspiration from nature and provides the best optimal results by solving problems numerically or mathematically. Exact and heuristic are two types of optimization techniques. Exact strategies work well for finding the optimal solution but, the complex problem requires a high computational cost. The Meta-heuristic approach able to solve many complex problems and helps to provide an optimal solution for most of the real-world problem. Various authors have provided detailed information about the meta-heuristic approach in several papers. Table 1 shows the different meta-heuristic approaches and the idea behind the approach.

Intensification and diversification are two important characteristics of meta-heuristic approaches. Intensification uses the information and searches around the neighborhood to find out the best solution whereas diversification explores more efficiently to find the best solution by randomization method. Many nature-based phenomena have specific characteristics that can be utilized to convert into mathematical equations and algorithms to solve many real-world problems. Over the last two decades, various nature-inspired algorithms like Genetic algorithm, artificial bee algorithm, particle swarm optimization etc are widely used by many researchers to find the best solutions. Yang in 2012 proposed a nature-inspired Flower Pollination Algorithm is based on the reproduction of flowers through pollination. Flower based algorithm is one of swarm optimization technique with impressive characteristics and fewer parameters like flexible, scalable, and simple optimization technique that provides robust performance. In recent studies, many researchers work on an initial version of FPA and to enhance its performance it has undergone modification and alterations. The FPA is considered as best to find optimized result

Electronic copy available at: https://ssrn.com/abstract=3358159

as compared to other algorithms. Meta-heuristic algorithms are inspired from nature provides different mathematical or numerical steps in order to solve optimization problems as per the special rules in accordance to natural systems. The main purpose of FPA is a reproduction of flower using pollination by insects, bats, wind, water etc.

The main objective of the paper is to implement secure and optimized technique. In this paper, we proposed a new hybrid flower pollination algorithm with DNA cryptography. Flower pollination algorithm is a nature-inspired algorithm that helps to find the optimal solution whereas DNA cryptography helps to encrypt a large number of data in few grams of DNA. In this paper, the original form of flower pollination algorithm is presented with DNA cryptography in order to achieve optimized technique to enhance cloud security.

Table 1 - Meta-heuristic algorithms and idea behind their inspiration.

Meta-heuristic Algorithms	Idea behind inspiration
Genetic algorithm (Goldberg, 1989)	Based on Drawin's theory
Ant colony optimization (Dorigo, et al., 1996)	Ants foraging behaviour
Flower Pollination (Yang, 2012)	Optimization using flower pollination behaviour
Bee Algorithm (Nakrani & Tovey, 2004)	Bees behaviour
Particle swarm optimization (Kennedy & Eberhart, 1995)	Social behavior of birds and fish
Bat Algorithm (Yang & Gandomi, 2012)	Echolocation behaviour of microbats

2. DNA Computing

Cryptography is an art of mathematical science for converting an original message into an unreadable form called encryption and convert it back to an original message called decryption. Advanced mathematical procedures are used to make more complex cryptography methods to protect data from unauthorized users. Cryptography offers a set of efficient solutions to protect sensitive information by encoding a message into cipher-text and decrypt it back into plain-text. Cryptography uses two main algorithms Symmetric and Asymmetric. Symmetric key uses same keys for encryption and decryption process and is low in cost also require limited resources Whereas, Asymmetric uses different keys for encryption and decryption and is computationally high in cost also uses more resources.

There are various types of cryptography methods that depend on the phenomena of nature. Modern cryptography is based on difficult mathematical equations and calculations such as matrix multiplication, prime factorization. Elliptical cryptography based on the elliptic curve problems. Quantum cryptography uses the randomness of the electron state inside the atom. DNA cryptography is based on the biological activity in DNA technology. Modern cryptography has adopted DNA cryptography as a new medium for encryption process. The DNA sequences have modified and give strength to the existing encryption techniques by adding more elements in confusion and diffusion process.

Every individual has unique DNA and the transmission of genes from one generation to another. DNA based algorithms are considered as revolutionary technique based on the surplus features such as large storage capability, ultra-low power consumption and massive parallelism (Yang, 2012). Leonard Adleman introduced DNA computing in 1994 at University of Southern California to solve the complex mathematical Hamiltonian problem in less time. Later on, Gahani et al., 2003 introduced DNA cryptography concept that is used by many researchers to improve data security methods. DNA constitution is based on Nitrogen Base, Pentose Sugar Molecule, Phosphate Molecule. Nitrogen bases are of four types.: A-adenine, G-guanine, C-cytosine, T-thymine. DNA base A forms pair with T and C forms a pair with G. DNA computing is an emerging technology that works on the concept of data security by hiding information in terms of the DNA sequence. DNA computing offers high storage and computational capabilities. The traditional existing algorithms such as RSA, AES, DES are used to achieve high security for data using encryption and decryption methods. The idea behind to convert plain text to DNA strand is its uncrackable characteristic. There are various DNA cryptographic method used by many researchers.

Hammami et al., 2018 proposed a new security concept that allows a users to transfer important data in the cloud. In the first phase, data is encoded into DNA nucleotides moreover mitigation and encryption done in the second phase. Sen et al., 2018 proposed DNA cryptography with the Diffie Hellman key-sharing technique for transmitting public key between the sender and receiver. Sukumaran et al., 2018 proposed DNA encryption algorithm based on bio-computational technique. For making a secure algorithm, steganography and indexing along with binary coding rule are used to increase computational complexity. Patnala et al., 2019 proposed DNA-based security algorithm uses DNA codons. It is a substitution method in which substitution is done using look table that contains DNA codons and equivalent alphabet values. The table is arranged randomly and transmitted to the receiver using a secure channel. Chai et al., 2019 presented dynamic DNA image encryption with a four-wing hyper-chaotic system. Siddaramappa et al., 2019 proposed a data security method based on DNA XOR operation. DNA cryptography with Genetic algorithm is proposed by Popli, 2018. In the first step, keys are generated using Genetic algorithm. Then, the plain text is converted in the form of a DNA sequence of nucleotides and at the end, encrypted data is again encrypted using the key to provide secure and unbreakable technique.

Electronic copy available at: https://ssrn.com/abstract=3358159

3. Flower Pollination Algorithm

Flower Pollination Algorithm is proposed by Xin-She Yang in 2012 (Mozaffari, 2018) inspired by the nature population. The main objective is to reproduce optimal plants by surviving the fittest plant. In nature, 80% of the plants are flowering species. It is typically related to the transfer of pollen by using pollinators such as insects, birds, etc. There are two major processes of pollen transfer one is Biotic or Cross Pollination and other is Abiotic or Self Pollination process. Biotic or cross-pollination occurs at a long distance where pollens are transmuted from one plant to other by a living organism such as insects, birds, etc. 90% of the pollens are from flowering plants and 10% are taken from the abiotic process. In Abiotic and Self Pollination that is also known as local pollination as in this impregnation in pollination of flowers from the same flower of the different flower of same plants with the help of wind or diffusion of water.

The originator of FPA Xin-she used four rules (Yang, 2012):

- Biotic cross-pollination can be viewed as a global pollination that obeys Levy flights patterns for carrying pollinators. [Rule 1]
- Abiotic self-pollination can be considered as local pollination. [Rule 2]
- The flower constancy that can be represented as reproduction ratio that is proportional to similarity of two flowers involved. [Rule 3]
- local and global pollination switching is controlled by a probability p ε [0,1] which is slenderly partial towards local pollination due to wind or water and physical proximity. [Rule 4]

The global pollinator is considered as the fittest and optimized pollinator that is carried by birds or insects as insects can travel long distance. Rule 1 can be formulated as mathematical shown in (1) in which g* is represented as fittest solution in current iteration.

$$x^{t+1} = x_i^t + \gamma L(g^* - x_i^t) \quad (1)$$

where x^t_i be the i^{th} pollen at t iteration, g* be the fittest solution in current iteration and L represents Lévy pollination step-size. The mathematical equation of Lévy distribution can be shown in (2)

$$L \approx \frac{\lambda \Gamma(\lambda)\sin(\pi\lambda/2)}{\pi} \cdot \frac{1}{s^{1+\lambda}} \quad (s >> s\,0 > 0) \quad (2)$$

where Γ(λ) denotes standard gamma function and distribution is legitimate for the large steps s>0. Local pollination and the flower constancy described in (Rule 2 & 3) can be mathematically formulated as shown in (3)

$$x_i^{t+1} = x_i^t + \varepsilon\left(x_j^t - x_k^t\right) \quad (3)$$

where x^t_i and x^t_k denotes the pollen from the same type of plant species of different flowers. If x^t_i and x^t_k are drawn from the uniform distribution then, it becomes a local random walk. Flower pollination can occur due to local or global. But in reality, adjacent flowers are more often pollinated then the flowers that are far. so the local pollination is more often happen then the cross-pollination. A switch probability, p ε [0,1] is used to switch between the common global pollination to local pollination. The naive value p=0.5 is used as an initial value but, exploratory parametric shows p=0.8 work better for most of the applications.

Flower pollination algorithm is procedurally an optimization technique that is initiated by a set of population. For each iteration one of the operations is carried out either global or local pollination. In global pollination, current solution variable is attracted to the globally best solution whereas, in local pollination, current solution variable attracts other randomly selected variables (Alyasseri, et al., 2018). The switch probability criteria are used to exchange loop between locally and globally until the predefined condition met. Though the standard flower pollination algorithm works well for various applications improvement is still required. Many researchers have discussed the modified version of FPA in order to enhance its performance.

Raouf et al., 2014 developed a hybrid flower pollination algorithm (FPPSO) that combines with the standard flower pollination algorithm with the particle swarm optimization to improve searching accuracy. Yamany et al., 2015 proposed a modified version of FPA based on the attribute reduction approach to choose the minimum number of attributes to obtain best or comparable classification accuracy from a set of all attributes. The aim of this paper is to obtain modified FPA by developing three initialization strategies forward and backward selection methods. Eight datasets from the UCI machine learning standards are utilized to obtain better performance. Dubey et al., 2015 proposed a hybrid flower pollination algorithm (HFPA) to solve dynamic multi-objective optimal dispatch (DMOOD) problem for a wind-thermal system for simultaneous minimizing cost, emission and power loss. Zhou et al., 2016 proposed an elite opposition-based flower pollination algorithm that includes two major optimization strategies Global elite opposition-based learning and local self-adaptive greedy. These strategies are applied to structural engineering problems and for function optimization. Global elite

Electronic copy available at: https://ssrn.com/abstract=3358159

opposition-based learning enhances population diversity and local self-adaptive greedy enhances the ability for exploitation. Abdelaziz et al., 2016 implemented FPA to solve ELD and CEED problems in power system. Economic Load Dispatch (ELD) allocate load between available generation units so that cost gets minimized. Combined Economic Emission Dispatch (CEED) considers the impact of emission of gaseous pollutants of fossil-fueled power plants in the environment. Pan et al., 2016 proposed a dynamic diversity flower pollination algorithm to solve multi-modal optimization problems.

Ram et al., 2017 proposed a hybrid Bee Pollinator Flower Pollination Algorithm for the PV parameter extraction problem. The proposed method is implemented via simplex method. Control variables are generated to evaluate the initial solution. Moreover, fitness values are obtained using an objective function to find the first best solution. Then based on the probability switch, global pollination or local pollination is performed. Local pollination is performed via elite based mutation process. Local pollination is performed by elite based mutation process. If fitness value fails to update the best solution then, the counter is incremented. Valenzuela et al., 2017 presented a new hybrid flower pollination algorithm that used a Fuzzy inference system for the impulsive change of switching probability. Pei et at., 2018 proposed a modified flower pollination algorithm that works in dual mode optimization. It also affects values of probability switching and population fitness and overcomes the defect of the local maximum in FPA. Zhang et al., 2019 constructed a collaborative service group-based fuzzy QoS-aware (CSGFQ) that describes QoS values using triangular fuzzy numbers. The extended version of flower pollination is used for algorithmic improvements effectively and efficiently.

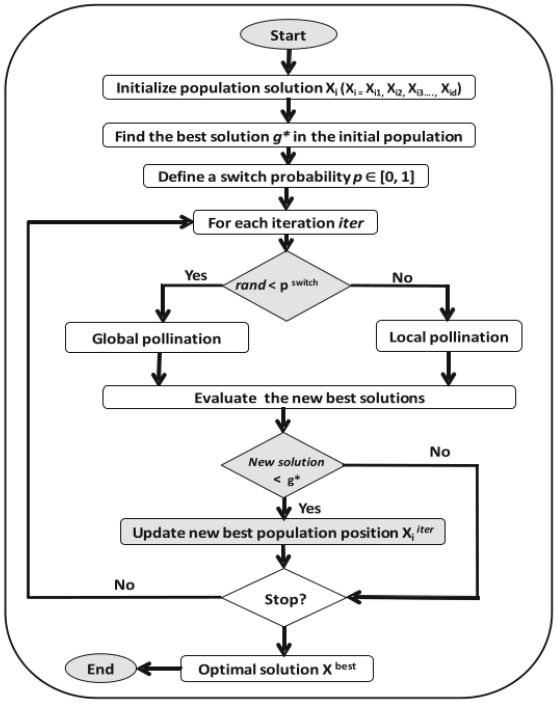

Fig 1: Flower Pollination Pseudocode

4. Proposed Work

This paper is an extended version of a paper presented by Popli, 2018. In this paper, data is encrypted using DNA cryptography along with the genetic algorithm. In this paper, plain-text is first converted into a set of DNA nucleotides and then re-encrypted using the key generated randomly from the genetic algorithm. Nature-inspired algorithms provide better optimal results as compared to the Genetic Algorithm. In this proposed work, the key is generated using flower pollination algorithm and data is encrypted using the key. Random generator assigns random sets of the DNA sequence of nucleotide bases (As, Cs, Gs, Ts) to the alphabets and numerical digits. The text is encoded into a DNA sequence that indicates a traditional computer can understand the randomly generated DNA sequence other than binary sequence. The DNA sequence is applied to each alphabet or number and a new sequence is generated. The randomly generated sequence of nucleotide bases is shown in table 2.

Electronic copy available at: https://ssrn.com/abstract=3358159

Table 2 - DNA sequence with respect to Alphabets and number.

ACCG - a	ATGG - n	TCCG - 0
TGCT - b	ATTC - o	AGGC- 1
CGTT - c	AGCT - p	ACCT - 2
TCGC - d	AGTC - q	TATC - 3
TGCA - e	CAGT - r	CAAT - 4
TGAC - f	CATG - s	TAGG - 5
TCGA-g	CTGA- t	TGGT - 6
TCAG - h	CTAG- u	CAAC - 7
TACG - i	CGTA - v	CGCG - 8
TAGC - j	CGAT - x	ATTA - 9
TAAG - k	GATC - w	GCTT - ‘ ’
GTAC - l	GACT - y	
GCAT - m	GCTA - z	

For example, the text “the world is here” is encoded in the form of DNA sequence as:

Step 1: T=CTGATCAGTGCAGCTTCGATATTCCAGTGTACTCGCGCTTTACGCATGGCTTTCAGTGCACAGTTGCA

Step 2: T=CTGATCAGTGCAGCTTCGATATTCCAGTGTACTCGCGCTTTACGCATGGCTTTCAGTGCACAGTTGCA

T’=GACUAGUCACGUCGAAGCUAUAAGGUCACAUGAGCGCGAAAUGCGUACCGAAAGUCACGUGUCAACGU

After the data gets encoded into a DNA sequence, it is then transcripted into a complementary strand. Complementary strand implies to replace the DNA nucleotide bases into complementary DNA (A → U, C→ G, G → C, T→ A). T represents the randomly generated sequence and T’ represents the complementary DNA sequence. The complementary DNA sequence table is shown in **Table 3.**

Table 3 - DNA Sequence in complementary form.

DNA Nucleotides Bases	Complimentary DNA
A	U
C	G
G	C
T	A

Step 3: T’ represents the complement of the DNA sequence. After converting into the complementary strand, a sequence is transformed into a binary sequence. The binary sequence for the nucleotides bases are shown in the table given below:-

Table 4 - Binary Sequence of DNA Nucleotides.

DNA Nucleotides Bases	Binary Sequence
U	11
C	01
G	10
A	00

Step 4: The binary sequence is further divided into blocks of 8-bit size.

T’=10000111 00101101 00011011 01100000 10011100 11000010 10110100 01001110 00100110 01100000 00111001 10110001 01100000 00101101 00011011 10110100 00011011

Electronic copy available at: https://ssrn.com/abstract=3358159

Step 5: Each byte is Right shift by 2 bits each

T'= 11100001 01001011 11000110 00011000 00100111 10110000 00101101 10010011 10001001 00011000 01001110 01101100 00011000 01001011 11000110 00101101 11000110

Step 6: Convert each byte in to decimal equivalent and divide each decimal number by key generated using Flower Pollination Algorithm

T'=10000111001011010001101101100000100111001100001010110100010011100010011001100000001110011011000101100000000101101000110111011010000011011

D=225 75 198 24 39 176 45 147 137 24 78 108 24 75 198 45 198

Step 7: Let key generated using flower pollination algorithm is -0.00897240006392. Operations are performed on the decimal numbers using key and result is stored in R. R is further converted into the hexadecimal form which will act as Cipher-Text.

The complete process of encryption using FPA is shown in **Fig 2**

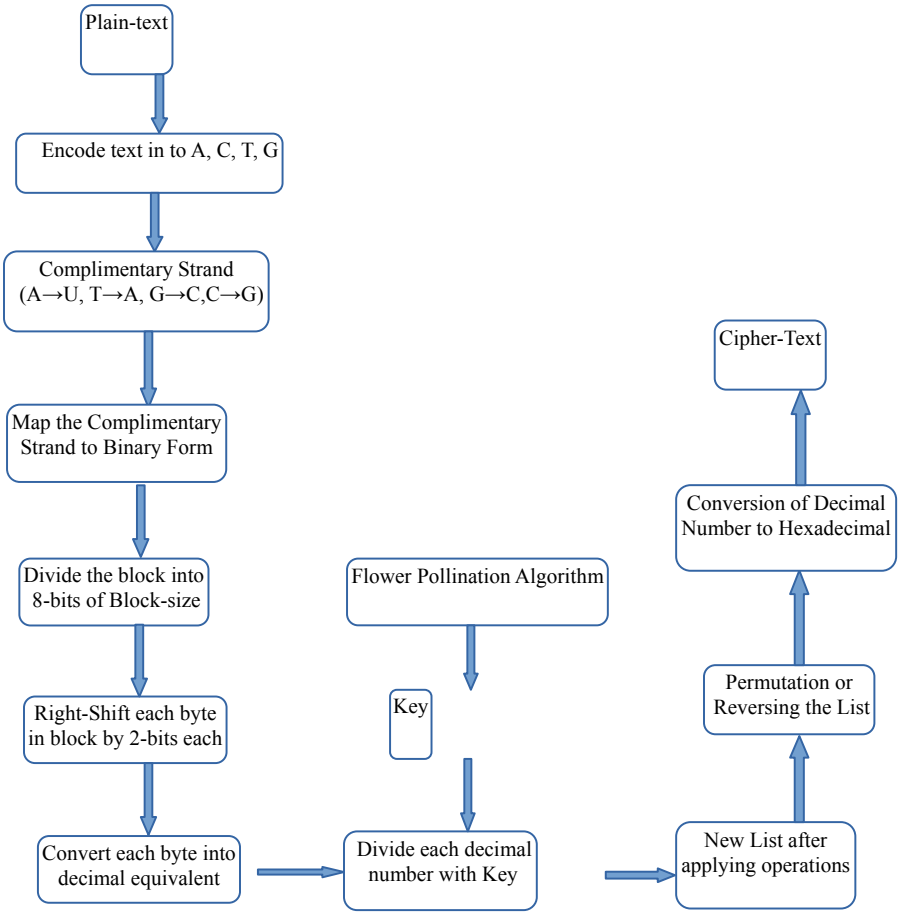
Plain-text
Encode text in to A, C, T, G
Complimentary Strand (A→U, T→A, G→C,C→G)
Map the Complimentary Strand to Binary Form
Divide the block into 8-bits of Block-size
Right-Shift each byte in block by 2-bits each
Convert each byte into decimal equivalent
Flower Pollination Algorithm
Key
Divide each decimal number with Key
New List after applying operations
Permutation or Reversing the List
Conversion of Decimal Number to Hexadecimal
Cipher-Text

Fig 2: Encryption Process

The complete description of the encryption process is demonstrated in figure 2. The algorithm is implemented using python. Random generator assigns random sets of the DNA sequence of nucleotide bases (As, Cs, Gs, Ts) to the alphabets and numerical digits.The encoded text is transformed into a complementary DNA sequence. It is further transcripted into binary form. Operations are performed to the DNA encrypted text using Key. Then, the text is further converted into encrypted and unbreakable form. The decryption process followed the reverse process.

Electronic copy available at: https://ssrn.com/abstract=3358159

5. Results and Conclusion

This paper is an extended version of a paper presented by author popli, 2018. In this paper, data is encrypted using DNA cryptography along with the genetic algorithm. In this paper, plain-text is first converted into a set of DNA nucleotides and then re-encrypted using the key generated randomly from the genetic algorithm. Nature-inspired algorithms provide better optimal results as compared to the Genetic Algorithm. In this proposed work, the key is generated using flower pollination algorithm and data is encrypted using the key. The nature-inspired FPA algorithm is used to obtain optimal results in minimum time. **Table 5** shows the encryption time of Paper presented by popli, 2018 and the time taken by proposed algorithm where as **Table 6** shows the decryption time taken by both algorithms.

Table 5 – Encryption Time

File Size	Paper[27]	Proposed Work
1 KB	0.0113	0.0011
2 KB	0.0243	0.0016
3 KB	0.0331	0.0020

Table 6 – Decryption Time

File Size	Paper[27]	Proposed Work
1 KB	0.0223	0.0015
2 KB	0.0420	0.0020
3 KB	0.0551	0.0030

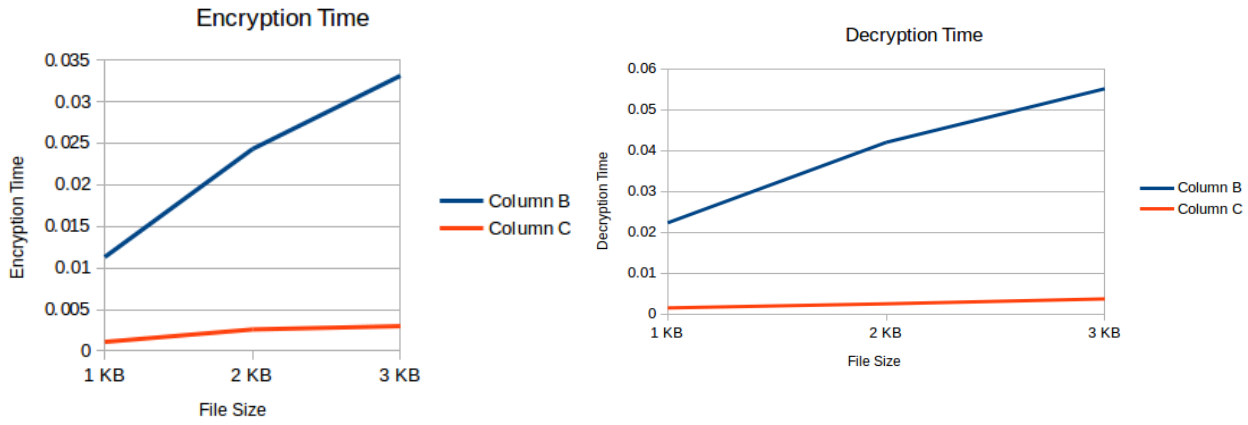

Fig 3: Encryption and Decryption Time taken by both algorithm.

The modern cloud technologies have changed the perspective of architecture, development and delivery models by providing on-demand services via the internet. With the extensive use of the internet, the risk of the number of threats is also increasing. It has become more difficult to secure important information from unwanted users. DNA cryptography plays a vital role in transforming important information into an encrypted form. In this paper, we proposed a new hybrid flower pollination algorithm with DNA cryptography. Flower pollination algorithm is a nature-inspired algorithm that helps to find the optimal solution whereas DNA cryptography helps to encrypt a large number of data in few grams of DNA. The proposed work is an extended version. The proposed work extends the level of security by implementing optimization including random key values. The work is entirely based on the random and optimized numbers so that no users can predict the level of randomization. The time complexity of the work shows the feasible nature of the algorithm.

Electronic copy available at: https://ssrn.com/abstract=3358159

Acknowledgements

This research is being carried out for Ph.D. work. I thank my supervisor Dr. Gagandeep for assisting me in improving this manuscript. I would like to show my gratitude to my supervisor for sharing her pearls of wisdom with me during the entire course of research work.

REFERENCES

Mell, P. , Grance, T., (2011). The NIST definition of cloud computing, Computer Security Division Information Technology Laboratory National Institute of Standard and Technology, pp 1-7.

Ravindran, A., Reklaitis , G. V., Ragsdell K. M. (2006). Engineering optimization: Methods and applications, Wiley.com.

Yang, X.S. (2012). Flower pollination algorithm for global optimization, Unconventional Computation and Natural Computation, Lecture Notes Computer Science, Springer, vol. 7445, pp 240–249.

Goldberg, David E. (1989). Genetic Algorithms in Search, Optimization and Machine Learning, Addison Wesley, Boston.

Dorigo, M., Maniezzo, V. , Colorni, A. (1996). Ant system: optimization by a colony of cooperating agents, IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), Vol. 26 , pp 29-41.

Nakrani, Sunil, Tovey, Craig (2004). On Honey Bees and Dynamic Server Allocation in Internet Hosting Centers, Adaptive Behavior, pp 223-240.

Kennedy, J., Eberhart, R. (1995). Particle swarm optimization, IEEE International Conference on Neural Networks, pp. 1942–1948, 10.1109/ICNN.1995.488968.

Yang, XS, Gandomi, A.H. (2012). Bat algorithm: a novel approach for global engineering optimization, Engineering Computations, Vol. 29, pp.464-483, 2012, https://doi.org/10.1108/02644401211235834.

Gehani, A, LaBean, T., Reif J. (2003). DNA-based cryptography, Aspects of Molecular Computing. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, pp 167–188.

Hammami, H., Brahmi, H., Yahia, SB. (2018). Secured Outsourcing Towards a Cloud Computing Environment Based on DNA Cryptography, IEEE International Conference on Information Networking (ICOIN), pp 31-36, doi: 10.1109/ICOIN.2018.8343079.

Sen, Alo, Roy, Rahul, Roy, Dash, SR (2018). Implementation of Public Key Cryptography in DNA Cryptography, Advances of DNA Computing in Cryptography, Taylor & Francis, pp 19-36.

Sukumaran, SC, Misbahuddin, M. (2018). DNA Cryptography for Secure Data Storage in Cloud, International Journal of Network Security, Vol. 20, No.3, pp.447-454.

Patnala, BD, Kumar R. K. (2019). A Novel Level-Based DNA Security Algorithm Using DNA Codons, In Computational Intelligence and Big Data Analytics, Briefs in Applied Sciences and Technology, Springer.

Chai, IXiuli, Fu Xianglong, Gan Zhihua, Lu Yang, Chen Yiran (2019). A color image cryptosystem based on dynamic DNA encryption and chaos, Signal Processing, Elsevier, Vol. 155, pp 44-62.

Siddaramappa, V. , Ramesh, K.B. (2019). DNA-Based XOR Operation (DNAX) for Data Security Using DNA as a Storage Medium, Integrated Intelligent Computing, Communication and Security, Studies in Computational Intelligence, Springer, Vol. 771, pp 343-351.

Popli, M. (2018), DNA Cryptography: A Novel Approach for Data Security Using Genetic Algorithm, International Journal of Advance Research in Computer Science and Management Studies,Vol.6, Issue 10.

Mozaffari, S. (2018). Parallel image encryption with bitplane decomposition and genetic algorithm. Multimedia Tools and Applications, Springer, pp 1-21.

Alyasseri Zaid Abdi Alkareem, Khader Ahamad Tajudin, Al-Betar Mohammed Azmi, Awadallah Mohammed A., Yang Xin-She (2018). Variants of the Flower Pollination Algorithm: A Review, Nature-Inspired Algorithms and Applied Optimization, Studies in Computational Intelligence, Springer, vol. 744, https://doi.org/10.1007/978-3-319-67669-2_5, pp 91-118.

Abdel-Raouf, Osama, Abdel-Baset, Mohamed, El-henawy, Ibrahim (2014). A New Hybrid Flower Pollination Algorithm for Solving Constrained Global Optimization Problems, International Journal Advanced Engineering Technology and Application, pp 21-28.

Yamany, Waleed, Zawbaa, Hossam M., Emary, E., Hassanien, Aboul Ella (2015). Attribute reduction approach based on modified flower pollination algorithm, IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), pp 1–7.

Dubey, HM, Pandit, M, Panigrahi B.K. (2015). Hybrid flower pollination algorithm with time-varying fuzzy selection mechanism for wind integrated multi-objective dynamic economic dispatch, Renewable Energy, Elsevier, Vol. 83, pp 188-202.

Zhou, Y., Wang, R., Luo, Q. (2016). Elite opposition-based flower pollination algorithm, Neurocomputing, Elsevier, Vol. 188, pp 294-310.

Abdelaziz, A.Y., Ali, E.S., Elazim, S.M.Abd (2016). Combined economic and emission dispatch solution using Flower Pollination Algorithm, International Journal of Electrical Power & Energy Systems, Vol. 80, pp 264-274.

Pan Jeng-Shyang, Dao Thi-Kien, Nguyen Trong-The, Chu Shu-Chuan, Pan Tien-Szu (2016). Dynamic diversity population based flower pollination algorithm for multimodal optimization, Proceedings of the 8th Asian Conference on Intelligent Information and Database Systems, Lecture Notes in Computer Science, Springer, vol. 9621, pp 440-448.

Ram J. Prasanth, Babu T. Sudhakar, Dragicevic Tomislav, Rajasekar N. (2017). A new hybrid bee pollinator flower pollination algorithm for solar PV parameter estimation, Energy Conversion and Management 135, Elsevier, pp 463-476.

Valenzuela L., Valdez F., Melin P. (2017). Flower Pollination Algorithm with Fuzzy Approach for Solving Optimization Problems. Nature-Inspired Design of Hybrid Intelligent Systems. Studies in Computational Intelligence, Springer, vol 667, pp 367-369.

Pei Tingting, Hao Xiaohong,Gu Qun (2018). A Novel Global Maximum Power Point Tracking Strategy Based on Modified Flower Pollination Algorithm for Photovoltaic Systems under Non-Uniform Irradiation and Temperature Conditions, Energies, pp 1-16.

Zhang Shuai, Yang Wenting, Zhang Wenyu, Chen Mingzhou (2019). A collaborative service group-based fuzzy QoS-aware manufacturing service composition using an extended flower pollination algorithm, Nonlinear Dynamics, Springer, https://doi.org/10.1007/s11071-018-04743-3, pp 1-24.

Electronic copy available at: https://ssrn.com/abstract=3358159